

ORIGINAL

AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. BRIAN NICHOLAS SIMONE		DOCKET NO.	
		MAGISTRATE'S CASE NO. 17-0973M	
Complaint for violation of Title 18, United States Code, Section 1708			
NAME OF MAGISTRATE JUDGE HONORABLE MICHAEL R. WILNER		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, California
DATE OF OFFENSE March 7, 2017	PLACE OF OFFENSE Los Angeles County	ADDRESS OF ACCUSED (IF KNOWN)	
COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION: <p style="text-align: center;">[18 U.S.C. § 1708]</p> <p>On or about March 7, 2017, in Los Angeles County, within the Central District of California, defendant BRIAN NICHOLAS SIMONE ("SIMONE") unlawfully possessed mail matter that had been stolen from the United States mail, namely, multiple pieces of mail addressed to various individuals within Los Angeles County, and at that time and place defendant SIMONE knew that said mail matter was stolen.</p>			
<div style="display: flex; justify-content: space-between;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg);"> LODGED MAY 2 2017 CLERK U.S. DISTRICT COURT CENTRAL DIST. OF CALIF. LOS ANGELES </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> CLERK U.S. DISTRICT COURT MAY 2 2017 CENTRAL DISTRICT OF CALIFORNIA DEPUTY </div> </div>			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: (See attached affidavit which is incorporated as part of this Complaint)			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT JARROD RESENDEZ		
	OFFICIAL TITLE Postal Inspector – USPIS		
Sworn to before me and subscribed in my presence,			
SIGNATURE OF MAGISTRATE JUDGE ⁽¹⁾ MICHAEL R WILNER			DATE May 2, 2017

⁽¹⁾ See Federal Rules of Criminal Procedure 3 and 54

AFFIDAVIT

I, Jarrod Resendez, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and an arrest warrant for BRIAN NICHOLAS SIMONE ("SIMONE") for Possession of Stolen Mail in violation of 18 U.S.C. § 1708.

2. This affidavit is also made in support of: (1) an application for a search warrant for 5460 White Oak Avenue, Unit K302, Encino, California (the "SIMONE HOME"), as further described in Attachment A-1; and (2) an application for a search warrant for a black Infiniti Q50s bearing an Infiniti of Van Nuys sticker and temporary identification number 35584326 located on the passenger side windshield (the "SIMONE CAR"), as further described in Attachment A-2. The requested search warrants seek authorization to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1704 (Possession of Counterfeit Postal Keys); 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail); 18 U.S.C. § 1029 (Access Device Fraud); and 18 U.S.C. § 1028A (Aggravated Identity Theft), as described more fully in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

II. BACKGROUND FOR POSTAL INSPECTOR JARROD RESENDEZ

3. I am a Postal Inspector ("PI") with the United States Postal Inspection Service ("USPIS") and have been so employed

Instrumentality Protocol

since August 2010. I am currently assigned to the USPIS Pasadena Mail Theft Team, where my responsibilities include the investigation of crimes against the United States Postal Service, crimes related to the misuse and attack of the mail system, theft of the United States mail ("US Mail"), possession of stolen US Mail, and crimes related to the use, theft, or counterfeiting of postal keys (referred to as "arrow keys") and locks. As part of the Mail Theft Team, I investigate crimes in connection with access devices, including crimes related to credit and debit cards, identity theft, and unauthorized use of personal identifying information, as these criminal schemes have been known to be perpetrated through the US Mail.

4. The Mail Theft Team also investigates crimes related to the use, theft, or counterfeiting of arrow keys and locks. From my training and experience, I know that arrow keys are keys used by USPS mail carriers to unlock USPS arrow locks, in order to gain access to housing complexes or apartment buildings and deliver mail to the respective mailboxes found inside—most commonly found in a mailbox panel. USPS arrow keys are also sometimes used to gain access to mail collection boxes in a specific area.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest

Instrumentality Protocol

warrant, and search warrants. It does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

6. On or about March 3, 2017, I received a mail theft complaint from the manager of a multi-unit condominium property in Encino. The manager informed me that surveillance video showed SIMONE, a resident of the complex, stealing mail from the mailroom. I reviewed the surveillance videos and also identified SIMONE as the mail thief based on his DMV photograph.

7. In the following weeks, I received complaints about mail theft from two other multi-unit properties in Encino. I reviewed surveillance videos from those properties and again identified SIMONE as the thief. At one of the properties, the video showed SIMONE arrive in the SIMONE CAR, steal mail, and then drive away. The SIMONE CAR has been parked in or near parking spaces assigned to the SIMONE HOME.

IV. STATEMENT OF PROBABLE CAUSE

A. Mail Theft Complaint at 5460 White Oak Ave

8. On or about March 3, 2017, I received a mail theft complaint from property manager C.W. at 5460 White Oak Ave, Encino. The complaint said that the mailboxes at the multi-unit condominium complex had been broken into. In the complaint,

Instrumentality Protocol

C.W. said that she reviewed surveillance video and identified the suspected mail thief as SIMONE, a resident at the property.

9. On or about March 3, 2017, I spoke with C.W. about the complaint. From that conversation I know the following:

a. C.W. explained that the community mailboxes for the property had been broken into multiple times. C.W. said on February 18, 2017, a resident reported that the mailbox panels were open and mail was exposed. C.W. added that on February 26, 2017, another resident notified her that the mailbox panels were open again. C.W. said the most recent incident occurred on March 2, 2017. C.W. said when she reviewed surveillance videos from February 26 and March 2, she identified SIMONE as the person who opened the mailboxes. C.W. said that the video showed him entering the gated mail area, using a key to open the mailbox panels, and stealing the mail. C.W. explained that she knows SIMONE is the sole tenant of the SIMONE HOME. C.W. also said that SIMONE's father or brother owns the SIMONE HOME.

10. On or about March 3, 2017, using law enforcement databases, I searched for SIMONE at the SIMONE HOME and found records confirming that he is associated with that address. I also requested and obtained a copy of SIMONE's Department of Motor Vehicles ("DMV") photo. On or about the same day, PI Preston Ellis and I met with C.W. to review the surveillance videos from February 26 and March 2, 2017. Based on my review of the surveillance videos I know the following:

Instrumentality Protocol

a. In the video dated February 26, 2017, the mail thief was wearing dark pants, a dark colored shirt, a dark colored Los Angeles Dodgers baseball hat, and white athletic shoes. The thief was carrying a dark colored bag. As he approached the gated mailroom, another person arrived at the property, and the thief, appearing to see the person arrive, walked away from the mailroom and towards the street. The thief later approached and entered the mailroom.

b. In the video dated March 2, 2017, the mail thief was wearing sunglasses, dark pants, a dark colored shirt, a dark colored Los Angeles Dodgers baseball hat and white athletic shoes. The thief also carried two dark colored bags. I saw the thief use a key to open the gated mailroom and approach the mailboxes. The thief then used a tool to open a single mailbox in the location corresponding to the mailbox for the SIMONE HOME. After the thief closed that single mailbox, I saw him open the mailbox panel.¹ Based on my training and experience, I know that when an unauthorized individual opens a mailbox panel, it is to steal mail.

11. After I reviewed the surveillance videos, C.W. gave me a document containing information about the SIMONE HOME. The

¹ From my training and experience, I know that "arrow keys" are keys used by United States Postal Service ("USPS") letter carriers to unlock USPS arrow locks, in order to gain access to housing complexes or apartment buildings and deliver mail to the respective mailboxes found inside-most commonly found in a mailbox panel. USPS arrow keys are also sometimes used to gain access to mail collection boxes in a specific area.

document listed SIMONE as the sole occupant of the condominium. C.W. explained that the SIMONE HOME has two parking spaces in the parking garage, numbered 602 and 603. PI Ellis and I went to the parking garage to inspect those parking spaces. In space number 604, directly adjacent to spaces 602 and 603, I saw a black Infiniti Q50s sedan with an Infiniti of Van Nuys sticker bearing temporary identification number 35584326 located on the front passenger side of the windshield. The vehicle did not have license plates, and instead had yellow Keyes dealership paper plates.

B. Mail Theft Complaint at 16542 Ventura Blvd

12. On or about March 13, 2017, I received a package from R.R., the property manager for 16542 Ventura Blvd, Encino. The package contained a mail theft complaint and surveillance video of a mail theft incident on March 7, 2017.

13. On or about the same day, I reviewed the surveillance video dated March 7, 2017. From my review of the video I learned the following:

a. On or about March 7, 2017, at approximately 4:56 p.m., a male carrying a black bag and wearing a dark colored striped shirt, dark colored pants, a dark colored Los Angeles Dodgers baseball hat, and white athletic shoes entered the parking garage and approached the mailboxes. The thief inserted an object into the mailbox panel and opened the entire door. He removed the mail and placed it in the black bag. He then moved to a nearby garbage can and rifled through the stolen mail. The

Instrumentality Protocol

suspect returned to the remaining mailboxes, opened each panel and removed the mail. The suspect closed the mailbox panels and left the area at approximately 5:11 p.m.

14. Based on my comparison of SIMONE's DMV photo with the mail thief in the video, I believe SIMONE is the thief.

15. On or about March 13, 2017, I called R.R., and he notified me about another mail theft on March 10, 2017. R.R. said he would send me the video surveillance from that theft.

16. On or about March 16, 2017, I reviewed the surveillance video from 16542 Ventura Blvd, Encino, dated March 10, 2017. From my review of the video I learned the following:

a. At approximately 11:27 a.m. on March 10, 2017, two men entered the parking garage and approached the mailbox units. Both men were wearing dark colored Los Angeles Dodgers baseball hats, sunglasses, and carrying black bags. The first thief was wearing a dark colored collared shirt, and grey colored pants and the second a black t-shirt and dark colored pants. The second thief had tattoos visible on his right arm.

b. The first thief approached the mailboxes, inserted an object into the mailboxes, and opened the mailbox panel. He removed mail and handed it to the second thief, who placed the mail in the first thief's bag. The second thief held a USPS Priority shipping box as the first thief opened a second mailbox panel and removed the mail. As the first thief removed the mail, he placed it in the shipping box that was held by the second thief.

Instrumentality Protocol

c. The second thief walked out of the camera's field of view as he was assembling a second USPS Priority Mail shipping box. The first thief remained at the mailboxes, removed keys from his pants pocket, used a key to open the mailbox panel, and removed more mail. At this point, the camera went dark. When the video resumed, both men were gone.

17. Based on my comparison of SIMONE's DMV photo and the first thief in the video, I believe SIMONE is the first thief.

C. Mail Theft Complaint at 16830 Ventura Blvd

16. On or about March 8, 2017, I received a mail theft complaint from N.M., property manager for 16830 Ventura Blvd, Encino. In the complaint, N.M. explained that on March 7, 2017, the complex's video surveillance showed a suspect using a key to open the mailboxes and steal the mail. On or about March 16, 2017, I reviewed the video surveillance provided by N.M. From my review of the video, I learned the following:

a. On March 7, 2017, at approximately 3:15 p.m., a black Infiniti sedan pulled into the loading area of 16830 Ventura Blvd. A man wearing sunglasses, a dark colored shirt, dark colored pants, white shoes, a dark colored baseball hat, and carrying a bag got out of the car. Shortly after leaving the car, the same man appeared on surveillance video from the mailroom. The man approached and opened multiple mailbox panels and stole the mail, placing it in the bag that he was carrying. In the mailroom video, I was able to see that the hat the man was wearing was a dark colored Los Angeles Dodgers baseball hat,

Instrumentality Protocol

and that he was wearing a striped shirt. After the man finished stealing the mail, he returned to the black Infiniti sedan and left the complex. The video from the loading area as the car drove away showed that it had a yellow rear license plate.

17. Based on my comparison of SIMONE's DMV photo and the man in the video, I believe SIMONE is the mail thief.

D. Follow-Up Investigation at 5460 White Oak Ave

18. On or about April 19, 2017, PI Carl Wright and I met with property manager T.H., at 5460 White Oak Ave, Encino to discuss my investigation. While at the property, I also met with postal letter carrier D.T. who was delivering the mail. D.T. opened the mailbox panel associated with the SIMONE HOME, and one of the names on the label identifying the people associated with that mailbox was "SIMONE."

19. After meeting with D.T., PI Wright and I walked to the resident parking garage to see if any cars were parked in spaces 602 and 603. We saw the SIMONE CAR parked in space 603, which is an assigned space for the SIMONE HOME.

20. Based on my review of the mail theft videos from the aforementioned locations and my comparison with SIMONE's DMV photo, I believe the mail thief depicted in each of the videos is SIMONE.

21. Based on the identification of SIMONE by property manager C.W., the condominium records listing SIMONE as the sole resident of the SIMON HOME, and my use of a law enforcement

Instrumentality Protocol

database, which associated SIMONE to the SIMONE HOME, I believe SIMONE lives at the SIMONE HOME

E. Identification of the SIMONE CAR

22. Based on the following, I believe that the SIMONE CAR belongs to and/or is used by SIMONE:

a. My observation on March 3, 2017 of the black Infiniti sedan with an Infiniti of Van Nuys sticker and temporary identification number 35584326 located on the passenger side windshield and yellow plates parked next to one of the parking spaces assigned to the SIMONE HOME.

b. My observation of SIMONE driving a black Infiniti sedan with yellow plates to and from 16830 Ventura Blvd, where I saw him steal mail on March 7, 2017.

c. My observation on April 19, 2017 of the black Infiniti sedan with Infiniti of Van Nuys sticker and temporary identification number 35584326 parked in space 603, which is assigned to the SIMONE HOME.

V. TRAINING AND EXPERIENCE IN MAIL THEFT INVESTIGATIONS

23. Based on my training and experience, including being a member of a USPIS Mail Theft Team, and information obtained from other law enforcement officers who investigate bank fraud and mail and identity theft, I know the following:

a. Persons who steal mail are often involved in fraud and identity theft crimes. These individuals usually steal mail looking for checks, access devices and personal identifying information that they can use to fraudulently obtain

Instrumentality Protocol

money and items of value. It is common practice for individuals involved in mail theft, access device fraud, and identity theft to use and maintain digital devices. These individuals use such devices to store information about their identity theft crimes during and long after the crimes have been committed. This information can include: logs of fraudulent transaction history; records of funds received; information regarding individuals and companies that have been victimized; records of payments from co-conspirators; and victim profiles. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

b. Mail and identity thieves oftentimes use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically on the internet. These individuals employ digital devices for purposes of, among other things, (i) applying online for fraudulent credit cards, (ii) obtaining personal identification information for the purposes of establishing or modifying fraudulent credit card accounts, (iii) using fraudulently obtained credit cards to make purchases, (iv) manufacturing counterfeit identification, credit cards, and checks, and (v) keeping records of their crimes.

Instrumentality Protocol

c. Based on my training and experience, I know that individuals who participate in these schemes often work with co-conspirators to steal mail, and to collect and use personal identifying and account information of their victims. These individuals often communicate by phone, e-mail, text message, and social media, sometimes exchanging information and photographs related to their crimes.

d. It is common for mail and identity thieves to keep the fruits, instrumentalities, and evidence of their crimes, such as stolen mail matter, in a place that is private, secure, and easily accessible, such as a residence or a car. This allows mail and identity thieves to comfortably sort through the stolen mail for items such as checks, money orders, credit cards, credit card applications, and other mail matter containing personal identifying information. Once mail and identity thieves obtain such stolen items, they can then further their criminal activity by, among other things, altering checks and other monetary instruments, fraudulently applying for credit cards, creating fraudulent identifications, and committing access device fraud.

e. It is also common for mail and identity thieves to keep "profiles" of victims in their residences, including on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state

Instrumentality Protocol

identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

f. It is also common for mail thieves, identity thieves, and individuals engaged in access device and identification document fraud to use equipment to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards.

g. Based upon my training and experience, and information related to me by other law enforcement personnel who specialize in the investigation of mail theft, I have learned it is common practice for individuals involved in such crimes to use and maintain computers at their residences and businesses. Such computers are used to track their fraudulent transactions. Suspects often use computers to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ computers for the purposes, among others, of:

(1) applying on-line for fraudulent credit cards; (2) obtaining personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; and (4) keeping records of their crimes.

Instrumentality Protocol

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

24. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. It is difficult to estimate the precise storage space contained on the devices listed in Attachment A before

Instrumentality Protocol

conducting a preliminary examination of these devices, but, based on my training and experience, I know that computers and cellular telephones can contain multiple gigabytes of storage space. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed

Instrumentality Protocol

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that

Instrumentality Protocol

show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a

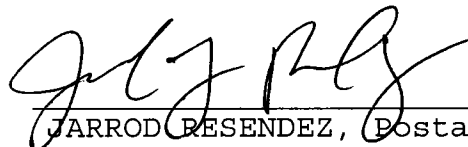
Instrumentality Protocol

controlled laboratory environment, and can require substantial time.

25. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

26. For the reasons described above, I respectfully submit that there is probable cause to believe that SIMONE violated 18 U.S.C. § 1708 (Possession of Stolen Mail), and that there is probable cause to believe that fruits, instrumentalities and evidence of violations of the offenses described above and in Attachment B of this affidavit, will be found at the SIMONE HOME and in the SIMONE CAR as further described in Attachments A-1 and A-2 of this affidavit.



JARROD RESENDEZ, Postal
Inspector
United States Postal Inspection
Service

Subscribed to and sworn before me
this 2nd day of May 2017


HONORABLE MICHAEL R. WILNER
UNITED STATES MAGISTRATE JUDGE

Instrumentality Protocol